Senate Committee on Commerce, Science and Transportation

Hearing on Unsolicited Commercial Email
May 21, 2003

Written testimony of Enrique Salem
President and CEO – Brightmail Inc.

Spam Problem Overview

Email has become a ubiquitous form of communication for both business and personal use. With email has come spam. Today, spam is spreading in such staggering amounts - flooding both corporate and personal inboxes - that it now threatens the viability of email as a primary communication tool. Unsolicited commercial email (UCE), commonly known as spam, has reached epidemic proportions. Analyst firm IDC currently estimates that 7.3 billion pieces of spam are sent each day with 3.9 billion of those sent in North America.

The growth curve has been steep. Over the last 5 years, we have seen the amount of unsolicited commercial email increase from a few messages to approximately 46% of all Internet email. Brightmail predicts that by December of 2003 spam will become more than 50% of all internet email. It has become a serious problem for Internet Service Providers (ISPs), businesses and individuals.

Unlike direct mail or telemarketing, email marketing has very low marginal cost. As a result, despite extremely low response rates, spammers can make a profit fairly easily. The more emails a spammer can send, the greater his profit, while the cost remains nearly constant. Bulk emailers are sending between 80 and 100 million messages a day. This both explains the alarming growth rate of spam and makes it more frightening - there is no financial disincentive for flooding the Internet with more and more spam.

Costs to ISPs and Businesses

A recent Gartner Group study on spam estimates that spam costs an ISP with 1,000,000 users $7 million per year. Spam is currently the number one complaint for many ISPs and is negatively impacting customer satisfaction while driving up support and infrastructure costs. Businesses are also not immune from the costs. A 2003 report by Ferris Research estimates that spam costs U.S. businesses $10 billion/year in lost productivity alone. Businesses must also add additional storage and bandwidth to handle the increase in email traffic due solely to spam. Lastly, businesses face an additional liability – allowing offensive and fraudulent content that is often a part of spam to reach employees. Adult content has increased more than 170% in the last 12 months and scams have nearly doubled in the same time period. These are concerns that go beyond the IT department and into the human resources arena.

Costs to Direct Marketers

Another significant consequence of the sheer volume of spam being sent is that over zealous filtering attempts are now blocking an increasing amount of legitimate mail. In many cases it is improperly deleted or placed in a bulk mail folder reducing the response rates to legitimate marketing campaigns.

Spam is a large and growing problem

As seen in Chart 1 below, Brightmail has seen an increase of more than 900% in the number of unique spam attacks/month from April 2001 to April 2003. A spam attack is a unique grouping of messages based on their content – for example, Herbal Viagra. Spammers will inject random content into each message to attempt to confuse filters by making each message that they send appear to be different. Attacks can have anywhere from ten to tens of millions of messages and can last from a few hours to many days.

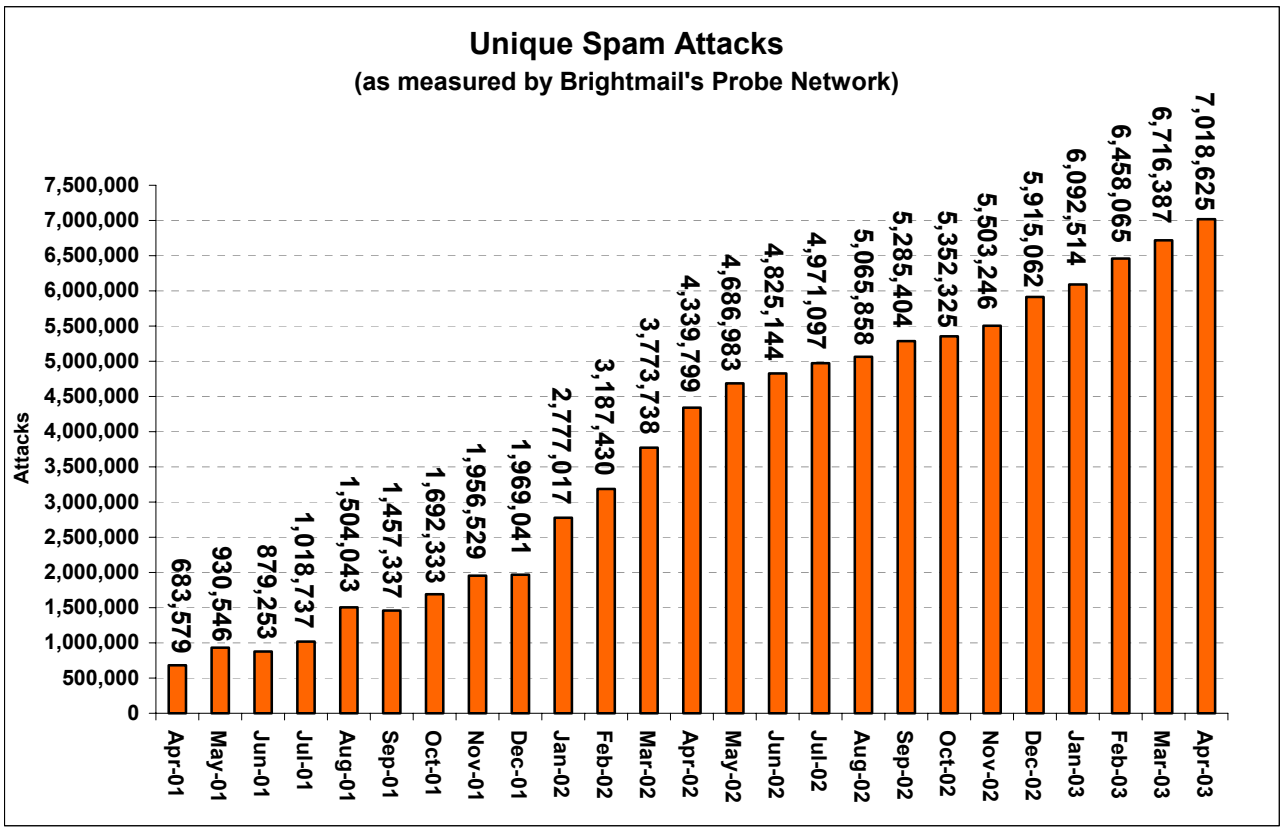
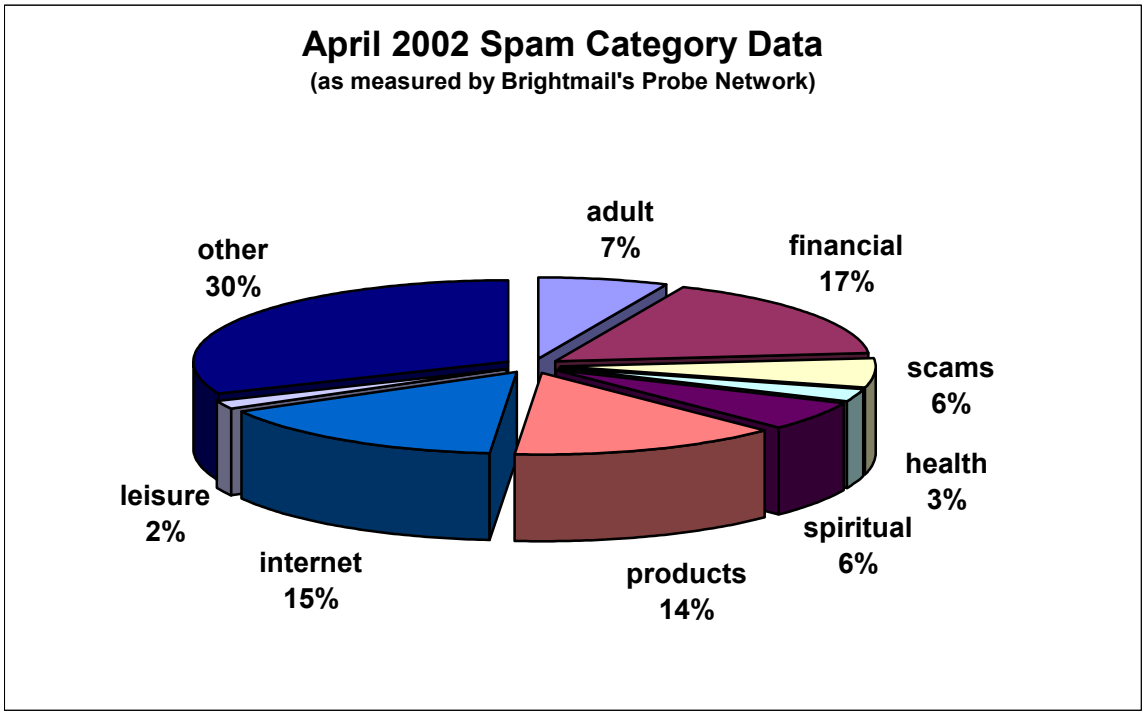
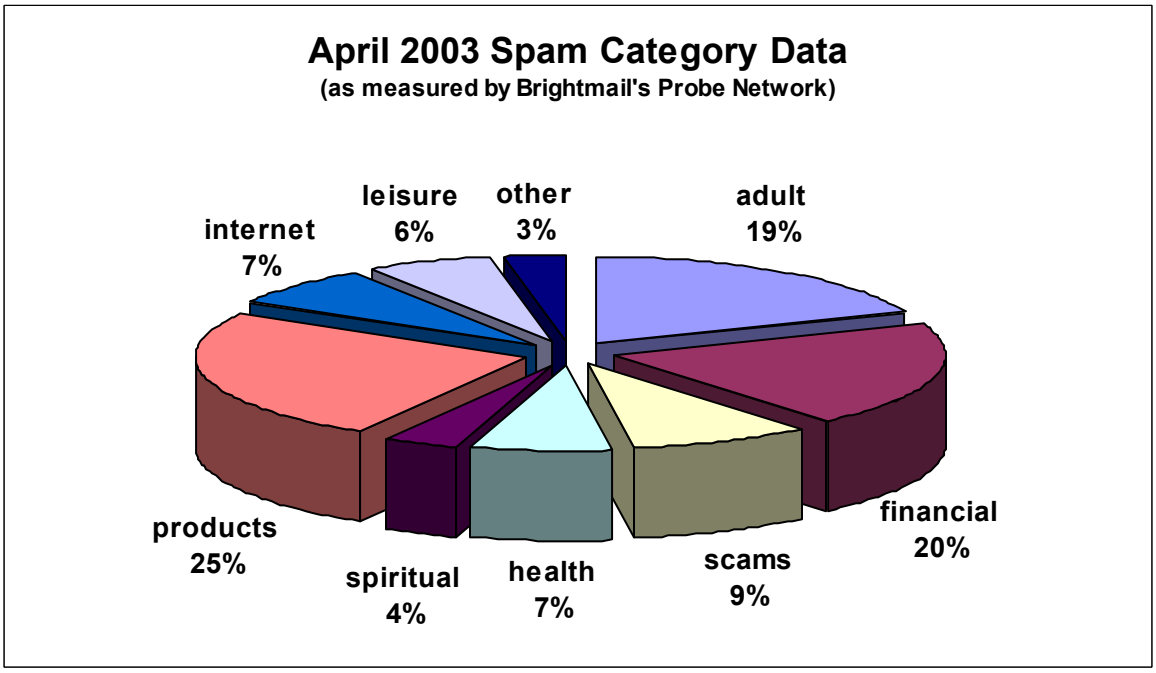


Chart 1

Spam is becoming increasingly offensive or fraudulent

As noted in Charts 2 and 3 below, from April 2002 to April 2003, Brightmail has seen "adult" spam increase by more than 170% and spam categorized as "scams" nearly double. These offensive emails are troublesome and costly for consumers as well as for businesses.





Charts 2 & 3

Spam is threatening the viability of email

As seen in Chart 4 below, over the past two years, both spam and email have grown. However, spam comprises a greater and greater percentage of the total amount of email that is sent each year, which is threatening the viability of email as a communications tool.

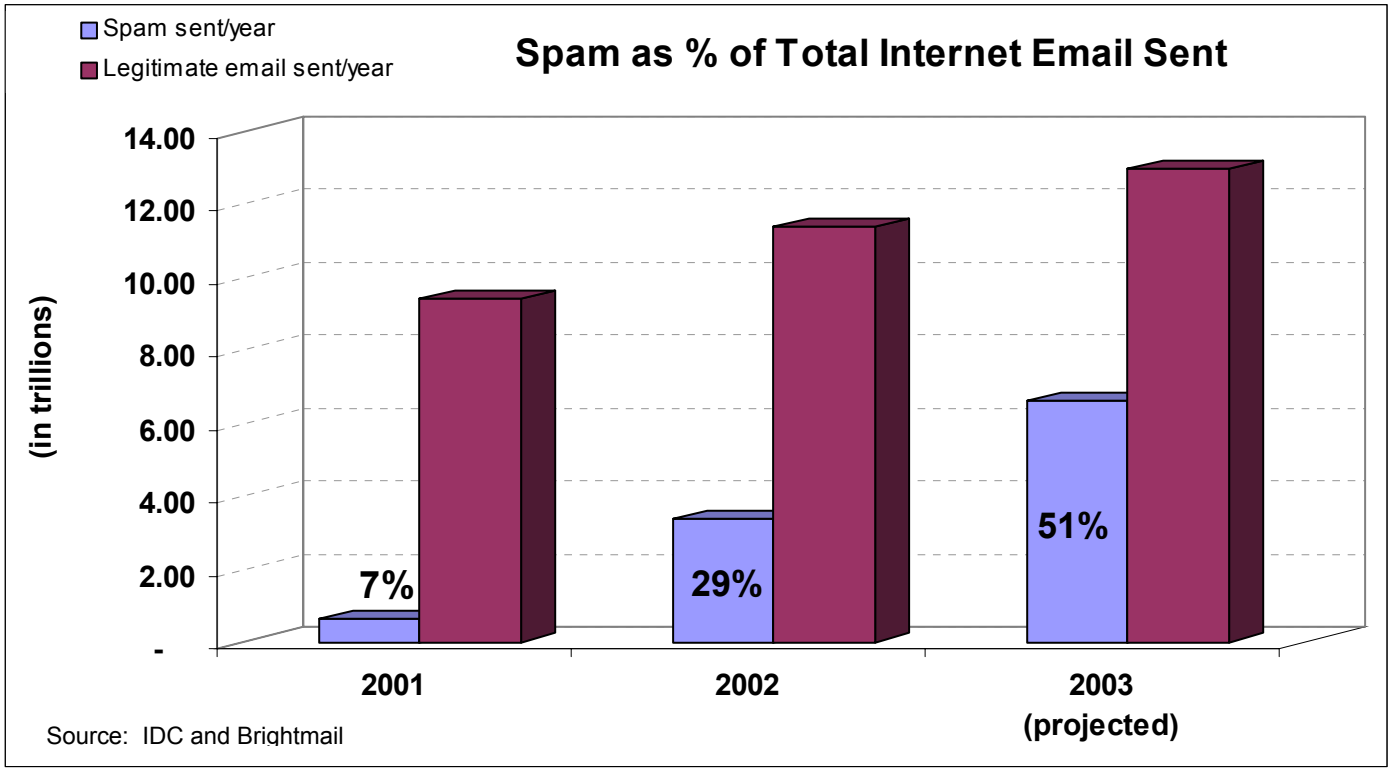


Chart 4

Spam is an International Problem

Much of the spam reaching U.S. inboxes is routed through other countries. The majority of spam is untraceable (90%), but of that spam that does claim to come from a certain region of the world, the majority comes from Europe – with the Russian Federation comprising 10% – and Asia – with China leading Asia. A key point to make is that even if a spam message claims to originate in China, it very well could have originated in North America or somewhere else. This point has implications as we consider the impact of various state and federal spam legislation.

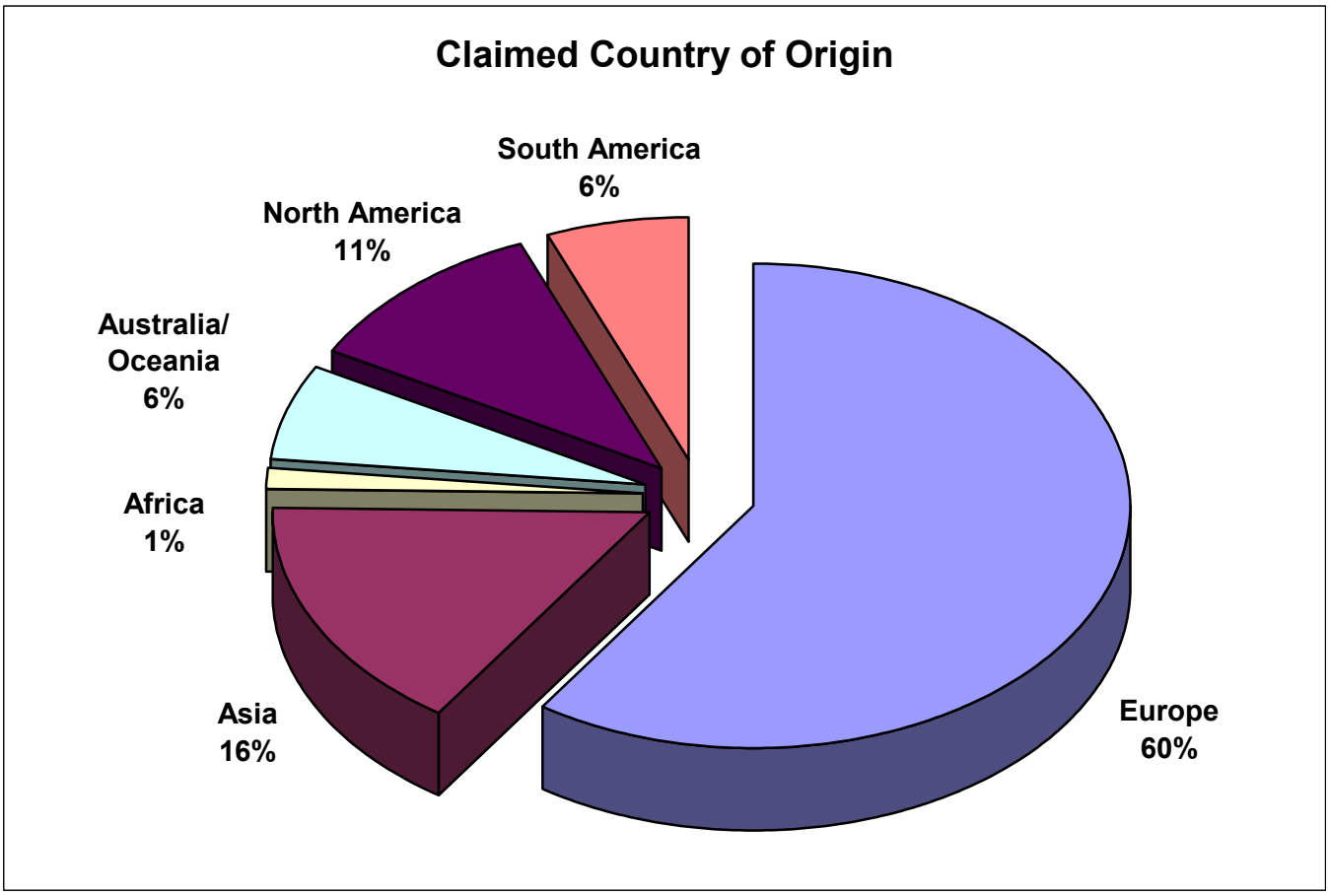
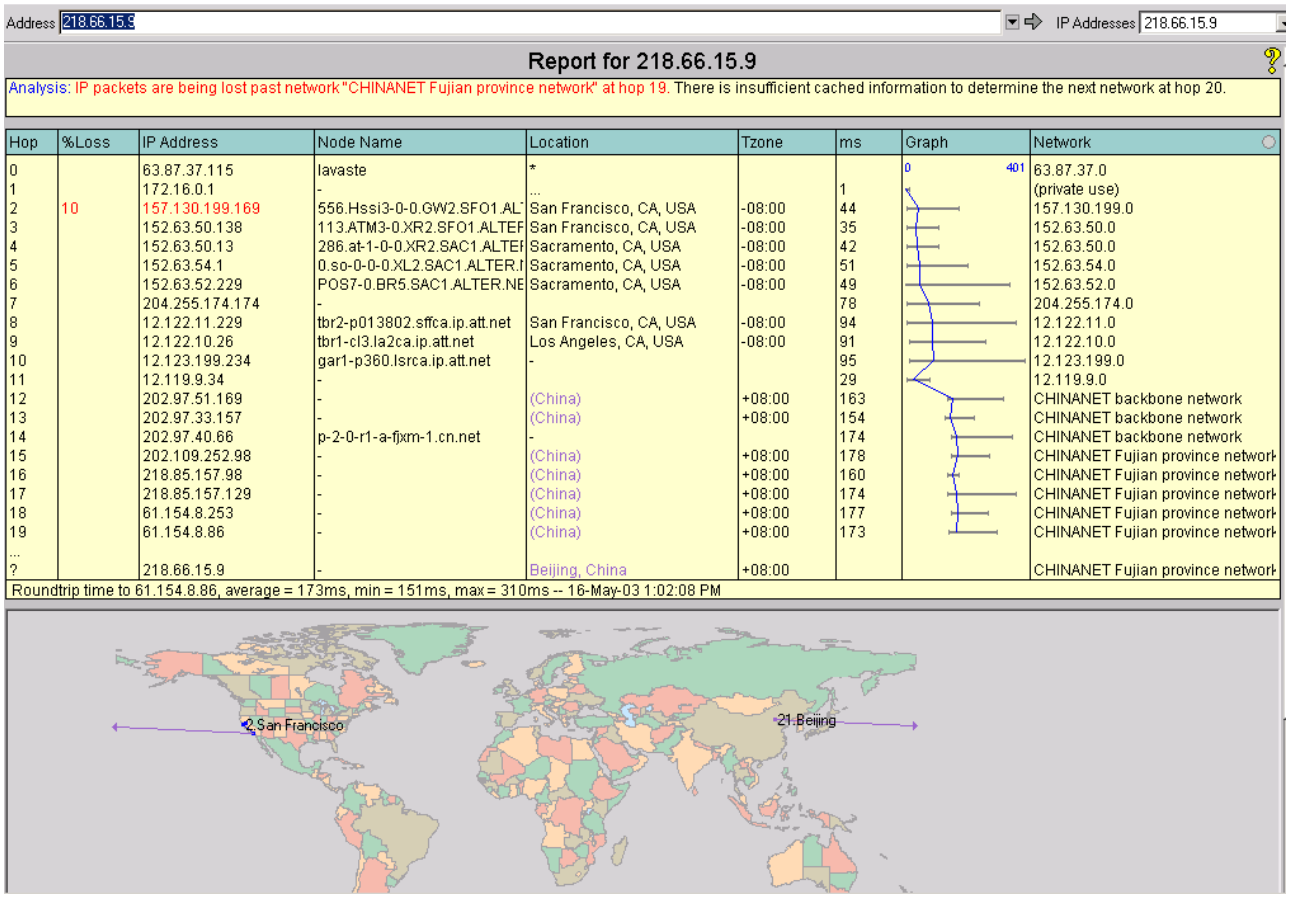


Chart 5

Tracking Spammers is difficult

Spammers often obfuscate their true location by enlisting open relays or proxy servers throughout the world. Trying to track down the true origin of a known spam message is often quite difficult, as demonstrated in Exhibit 1 below.



Address 218.66.15.9 IP Addresses 218.66.15.9

Report for 218.66.15.9

Analysis: IP packets are being lost past network "CHINANET Fujian province network" at hop 19. There is insufficient cached information to determine the next network at hop 20.

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph (0 – 401)	Network
0		63.87.37.115	lavaste	*				63.87.37.0
1		172.16.0.1	-	...		1		(private use)
2	10	157.130.199.169	556.Hssi3-0-0.GW2.SFO1.AL	San Francisco, CA, USA	-08:00	44		157.130.199.0
3		152.63.50.138	113.ATM3-0.XR2.SFO1.ALTEF	San Francisco, CA, USA	-08:00	35		152.63.50.0
4		152.63.50.13	286.at-1-0-0.XR2.SAC1.ALTEF	Sacramento, CA, USA	-08:00	42		152.63.50.0
5		152.63.54.1	0.so-0-0-0.XL2.SAC1.ALTER.I	Sacramento, CA, USA	-08:00	51		152.63.54.0
6		152.63.52.229	POS7-0.BR5.SAC1.ALTER.NE	Sacramento, CA, USA	-08:00	49		152.63.52.0
7		204.255.174.174	-			78		204.255.174.0
8		12.122.11.229	tbr2-p013802.sffca.ip.att.net	San Francisco, CA, USA	-08:00	94		12.122.11.0
9		12.122.10.26	tbr1-cl3.la2ca.ip.att.net	Los Angeles, CA, USA	-08:00	91		12.122.10.0
10		12.123.199.234	gar1-p360.lsrca.ip.att.net	-		95		12.123.199.0
11		12.119.9.34	-			29		12.119.9.0
12		202.97.51.169	-	(China)	+08:00	163		CHINANET backbone network
13		202.97.33.157	-	(China)	+08:00	154		CHINANET backbone network
14		202.97.40.66	p-2-0-r1-a-fjxm-1.cn.net	-		174		CHINANET backbone network
15		202.109.252.98	-	(China)	+08:00	178		CHINANET Fujian province network
16		218.85.157.98	-	(China)	+08:00	160		CHINANET Fujian province network
17		218.85.157.129	-	(China)	+08:00	174		CHINANET Fujian province network
18		61.154.8.253	-	(China)	+08:00	177		CHINANET Fujian province network
19		61.154.8.86	-	(China)	+08:00	173		CHINANET Fujian province network
...								
?		218.66.15.9	-	Beijing, China	+08:00			CHINANET Fujian province network

Roundtrip time to 61.154.8.86, average = 173ms, min = 151ms, max = 310ms -- 16-May-03 1:02:08 PM

Exhibit 1

Use of Open Proxies

Spammers aggressively use technology to hide their tracks. A perfect example is the growing use of open proxies; open proxies are misconfigured servers that allow spammers to generate large volumes of email that are not easily traceable to the actual sender. There are many thousands of open proxy servers available to spammers at any given time and a great deal of spam flows through these servers – both in the U.S. and overseas.

Changing Techniques to Reach Inboxes

Spammers have moved beyond simple text-based email to entice end-users to click through. One such technique is using HTML-based email. An example of a recent HTML-based spam message appears to the recipient as follows:

Exhibit 2

When in reality, the HTML code behind this seemingly benign image is collecting valuable information for the spammer.

Pulls info down from URL and provides feedback to spammers!

```
<BR><BR></FONT></DIV>
<DIV align=center>
<P><A
href="http://www.info@abc-
deals1.com/cellbooster/welcome11.html?affid=1000&amp;e=info@brightlight.com">
<IMG
height=340 src="http://210.22.144.195/cbgraphics.jpg" width=468 border=0
NOSEND="1"></A>
<P><A href="http://210.22.144.195/r/?e==info@brightlight.com"><IMG height=20
src="http://210.22.144.195/re.gif" width=209 border=0
NOSEND="1"></A><BR>"Why
aren't you in a more interesting business?"<BR>`Yes,' said Arthur, `yes I did.
It was on display in the bottom of a locked filing cabinet stuck in a disused
lavatory with a sign on the door saying "Beware of The Leopard".'"
</FONT></P></DIV></BODY></HTML>
```

Random text inserted by spammer tools

Spam Can Lead to Digital Identity Theft

Spammers also employ well-known brand names in an attempt to get end-users to open emails. Not only does this perpetrate the spam problem, it also does considerable damage to the reputations of companies.

We see spam from global corporations that was actually sent out by a spam shop halfway around the globe. These innocent corporations face more than the wave of bounced messages and angry responses from the spammed. This type of corporate identity theft can severely damage a company's worldwide brand since spammers have global reach.

Additionally, some misguided attempts to fight spam result in building blacklists that often include the domain names of these victims of domain identity theft. These blacklists further the damage done by the open relays and falsified headers of spammers when subscribers to these blacklists can no longer receive email from the legitimate enterprises. Domain names are an intrinsic part of a corporate brand. The theft of these names for mass mailing of unsolicited email has hurt some companies already and the trend may grow in the months and years ahead.

Corporations have a responsibility to their employees and shareholders to take measured steps in securing their messaging systems. In fact, as liability cases do make their way into the courts, the extent to which corporations can demonstrate that they made "best efforts to protect against spam" will have a large bearing on the outcomes.

In the header information in Exhibit 3 below, a spammer has used two well-known company names to trick the recipient into thinking that the email is from a trusted source, when in fact it is just an attempt to obfuscate the true identity of the sender.

From: "Chase S. Stewart" cs_stewart@fedex.com
To: xyz123@hotmail.com
Subject: Whatever works better
Date: Wed, 26 Mar 2003 13:05:01 +0000
MIME-Version: 1.0
Received: from 3com.com ([218.62.7.234]) by mc4-f42.law16.hotmail.com with Microsoft SMTPSVC(5.0.2195.5600); Wed, 23 Apr 2003 02:09:59 -0700
X-Message-Info: JGTYoYF78jEHjJx36Oi8+Q1OJDRSDidP
Message-ID: <HJHOBIKCNELIIEBKOCHFFLPADPAB.cs_stewart@fedex.com>
In-Reply-To: <d21101c2f1b6$db026239$9d8010e0@4e5d6bz>
X-MIMEOLE: Produced By Microsoft MimeOLE V6.00.2800.1106
X-Mailer: Microsoft Outlook IMO, Build 9.0.2416 (9.0.2910.0)
Return-Path: cs_stewart@fedex.com
X-OriginalArrivalTime: 23 Apr 2003 09:10:03.0620 (UTC)
FILETIME=[20200240:01C30978]

Exhibit 3

Spam: Moving Beyond Email

Wireless Spam

There is a huge impending need for anti-spam protection in the mobile/wireless environment. Wireless email produces a unique set of threats from spam, including volume issues when wireless users receive large amounts of spam. Viruses and worms can harm or temporarily paralyze PDA devices or the applications that run on them. Cell phones are particularly vulnerable to dictionary attacks done by spammers using phone numbers, with the advent of text messaging and SMS.

There is currently more of a need for anti-spam protection for wireless devices in foreign markets than in the U.S. The highest risk to wireless spam and viruses exists in Asia and Europe, but the need in the U.S. for protection is growing. We can see the future for U.S. wireless in overseas experiences as they have adopted wireless technology more rapidly. One way that spam is affecting wireless communications overseas is by causing carriers to pay back their own customers for each spam message received. Since carriers like NTT DoCoMo in Japan charge for incoming messages, customers were at first paying their carrier for the pleasure of receiving and having to delete spam from their own devices. Now DoCoMo refunds customers for spam messages received, which is detrimental to DoCoMo's bottom line.

Additional costs of wireless spam are passed on to end-users. With wireless messaging pricing models, wireless users must pay for each message and, often, each line of content within that message. With unwanted messages flooding wireless devices, end-users will no longer find technologies like SMS a viable mode of communication. With the continued adoption of wireless communications in the U.S. will come a dramatically increased need for wireless anti-spam and anti-virus technology, to protect the end user and the provider's bottom-line. As wireless adoption continues, spammers will increasingly target wireless users with spam, making for an expensive and very inconvenient dilemma. As spam invades PDAs, cell phones and the like, wireless carriers will have to block spam or face customer churn and costly refunds for unwanted wireless spam.

Instant Messaging (IM) Spam

Spam is also infiltrating the desktops of business and home users via another popular communication tool – Instant Messaging (IM). As more businesses use IM to communicate with business colleagues who are offsite or traveling, spam via this route has some of the same negative impacts that it does via email – productivity issues and potential liability issues for offensive content that is delivered via IM.

Exhibits 4 and 5 below are examples of recent IM spam that were received by business users. Exhibit 4 offers a common pitch to lose weight while Exhibit 5 contains more offensive content. Spam via IM is of particular concern to parents whose children use IM to communicate with friends.

Exhibit 4:

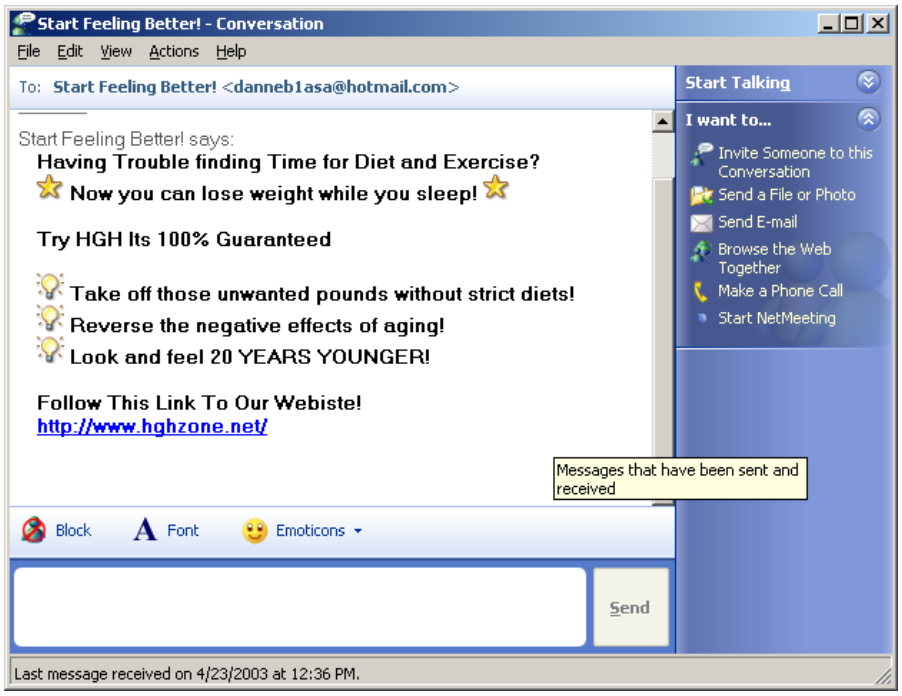
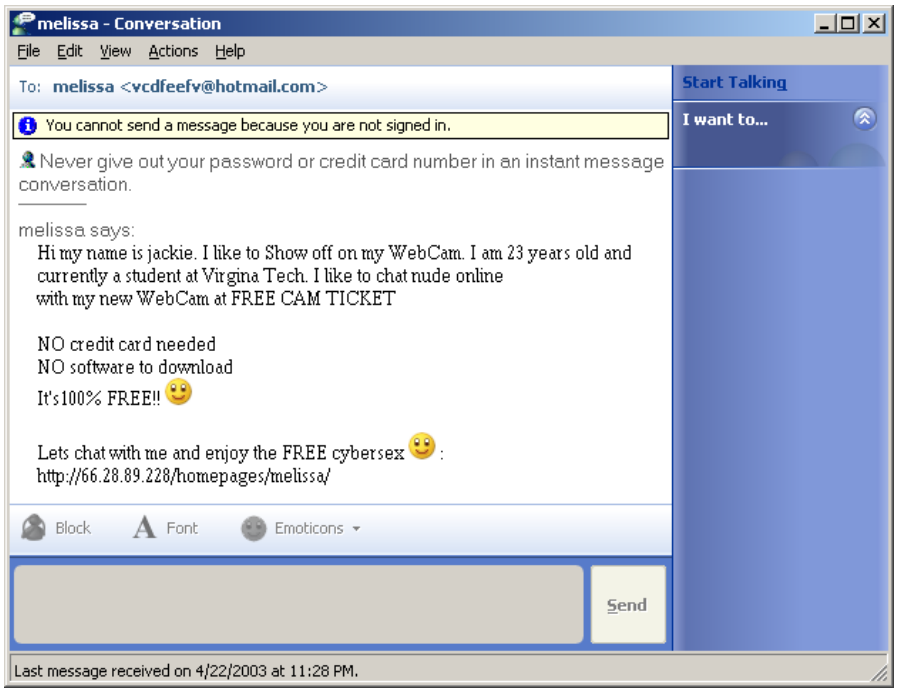


Exhibit 5:



Impact of Current Spam Legislation

State Legislation

As of April 2003, twenty-nine (29) states have spam control laws. In July 1997 Nevada became the first state to enact spam control legislation (law amended in 2001 and 2003). Nevada law states that it is illegal to send unsolicited commercial e-mail unless it is labeled "ADV" or "ADVERTISEMENT" at the beginning of the subject line, and includes the sender's name, street address, and e-mail address, along with opt-out instructions.

Similar spam control legislation was passed in California in September 1998. California law currently states that unsolicited commercial e-mail messages must include opt-out instructions and contact information, and opt-out requests must be honored and that certain messages must contain a label ("ADV:" or "ADV:ADLT") at the beginning of the subject line. Only a small percentage of the messages Brightmail processes each month uses these labels, partly because less sophisticated spam filters were identifying messages with these marks and partly because spammers do not abide by these U.S. state laws since they are not sending spam from these states

Indiana and New Mexico and Virginia are the states to most recently pass spam related legislation, doing so in April 2003. Virginia's recently updated law has received a great deal of attention due to the stiff penalties for sending spam from within the state of Virginia, including giving the authorities power to seize assets earned from sending bulk unsolicited email pitches while imposing up to 5 years in prison for violators.

Have these state laws had an impact on the volume of spam? Not really – spam has continued to increase dramatically over the past few years, from being an annoyance to a serious threat to the viability of email. Part of the problem has to do with enforcement of the laws – there have been limited number of cases that leverage current state law given that the burden of proof is often on the recipient and can be a heavy burden at best. An example of this heavy burden is the eTracks case that is currently being litigated by a San Francisco-based law firm, Morrison and Foerster LLP. States have limited budgets and those dollars are being allocated to enforcing laws that more directly impacts the safety and well being of its residents.

Foreign Spam Legislation

We've seen spam legislation enacted in other countries, such as Japan where businesses delayed implementing technological solutions in hopes that federal legislation would eliminate the spam problem. The law, enacted in October 2002, which required unsolicited text messages to be tagged, has had little impact on reducing the volume of spam sent via text messaging in Japan.

The European Union (EU) has also passed legislation that its member states must comply with by October 2003, which requires that there must be a prior opt-in relationship between a sender and recipient in order for unsolicited email or text messaging to be sent. Some member states are already in compliance, but the amount of spam that European email users receive continues to climb. ISPs and European businesses are being forced to examine technological solutions to the spam problem, given that legislation is having little impact on the spam problem.

Federal Spam Legislation

There is hope that federal laws will have the muscle required to combat the growing spam problem. The only current federal restrictions on email spam are the general criminal and civil fraud prohibitions. The FTC currently works with law enforcement to combat fraudulent email scams, but at the moment 56% of spam does not fit the legal definition for fraud, according to a recent study by the FTC, and is therefore beyond current law. Given federal, state, and local law enforcement's focus on preventing terrorism and their limited resources, they simply cannot keep up with spam.

However, there are a number of proposals currently in front of Congress.

These include the Can Spam Act (revised in April 2003) that would require unsolicited commercial e-mail messages to be labeled, require unsolicited commercial e-mail messages to include opt-out instructions and the sender's physical address, and prohibit the use of deceptive subject lines and false headers in such messages. Additionally, this bill would pre-empt any state laws that prohibit unsolicited commercial e-mail outright, but would not affect the majority of state spam laws.

Another Federal initiative, the Computer Owners' Bill of Rights (S. 563) would require the Federal Trade Commission to establish a "do-not-email" registry of addresses of persons and entities who do not wish to receive unsolicited commercial e-mail messages. Additionally, the FTC would be empowered to impose civil penalties upon those who send unsolicited commercial e-mail to addresses listed on the registry.

A third proposed law, the Reduce Spam Act, requires that unsolicited bulk commercial e-mail messages would be required to include a valid reply address and opt-out instructions, and a label ("ADV:" or "ADV:ADLT", or other recognized standard identification). These requirements would apply to messages sent in the same or similar form to 1,000 or more e-mail addresses within a two-day period. In addition, false or misleading headers and deceptive subject lines would be prohibited in all unsolicited commercial e-mail messages, whether or not sent in bulk.

Additionally, New York Senator Charles Schumer is planning to propose legislation that would incorporate many elements of other proposed legislation but also adds funding for enforcement of the "do not mail" registry component of his proposed legislation.

From our point of view labeling has not helped to solve the problem, as it is a component of current state legislation.

Benefits and Consequences of Legislation

As with other public hazards, legislation can play an important role in the fight against spam. However, the extent of the problems often extends beyond state and country borders, preventing legislation alone from solving the problem. Consider the parallels in the offline world. While there are many "laws of the road" for drivers, still the public wants the auto industry to build as many safety features into cars as they possibly can. Similarly, while "Breaking and Entering" is a felony crime, homeowners use locks, bars and alarm systems to protect themselves from robbery.

While legislation plays an important role in highlighting the seriousness of spamming, it is currently very difficult to enforce. Spamming is a global problem, with email being routed around the globe and with wanton disregard for local regulations. Governments cannot impose regional laws on assailants outside their boundaries. Even when legal authorities can catch a spammer within their jurisdiction, the burden of proof can be daunting to prosecuting attorneys.

Legislation may help to deter some spammers and provides a framework for prosecution and operations of both Direct Marketers and anti-spam companies. But, enforcement is key and will prove expensive and difficult. We need to alert this committee that is it critical to set the expectations of the public at the right level as far as the real impact of legislation on the volume of spam received.

We believe the solution will involve a coordinated effort by Internet Service Providers, Direct Marketers, technology providers and law enforcement agencies. We will need to establish guidelines that outline email best practices. These guidelines will need to be followed by direct marketers. It will become important to be able to identify legitimate direct marketers and there will need to be improvements in how direct marketers manage their lists.

Appendix

Brightmail Corporate Overview

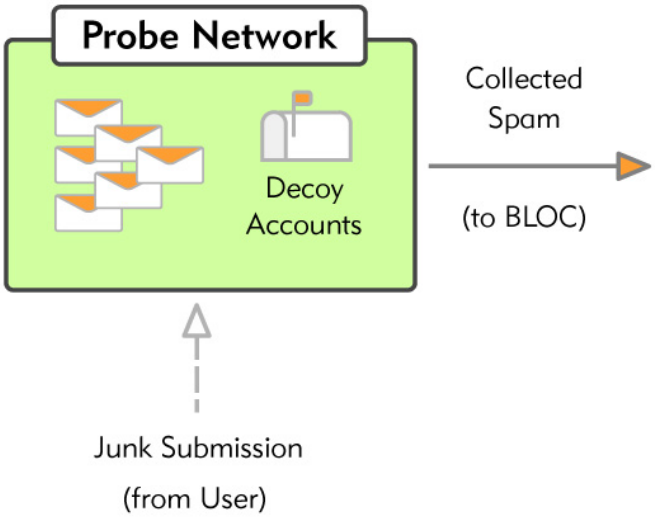
Brightmail, the worldwide leader in anti-spam technology, provides anti-spam software that makes messaging secure and manageable. Founded in 1998, Brightmail protects the networks of enterprises, service providers, and mobile network operators by filtering spam, viruses and undesired messages at the Internet gateway. Brightmail currently serves many of the largest service providers, including AT&T WorldNet, EarthLink, MSN, and Verizon Online as well as leading enterprises that include eBay, Booz Allen Hamilton, Deutsche Bank, and Cypress Semiconductors.

In April 2003, across its customer base, Brightmail software filtered over 60 billion messages and protected over 250 million mailboxes.

Brightmail anti-spam architecture includes a patent protected "spam alert network" called the Brightmail Probe Network, a collection of more than a million decoy email accounts. It is designed to attract unsolicited email and has a statistical reach of more than 250 million email accounts that provide Brightmail with a unique insight into the changing face of spam throughout the world.

Brightmail is backed by world-class investors and partners and is headquartered in San Francisco, CA.

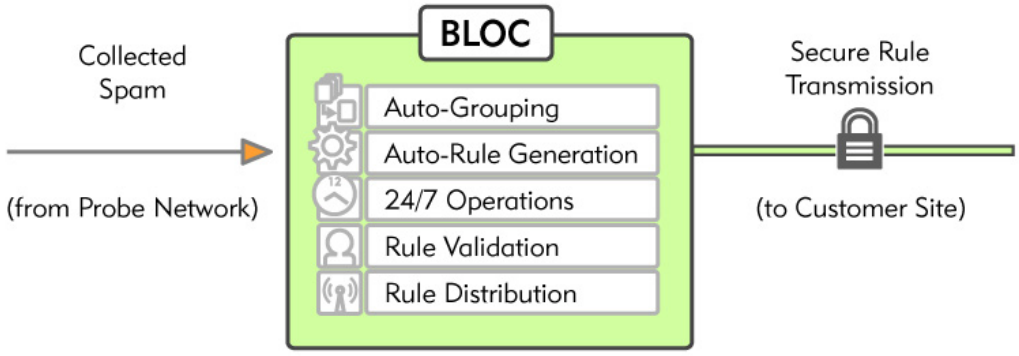
Brightmail Architecture



Probe Network™

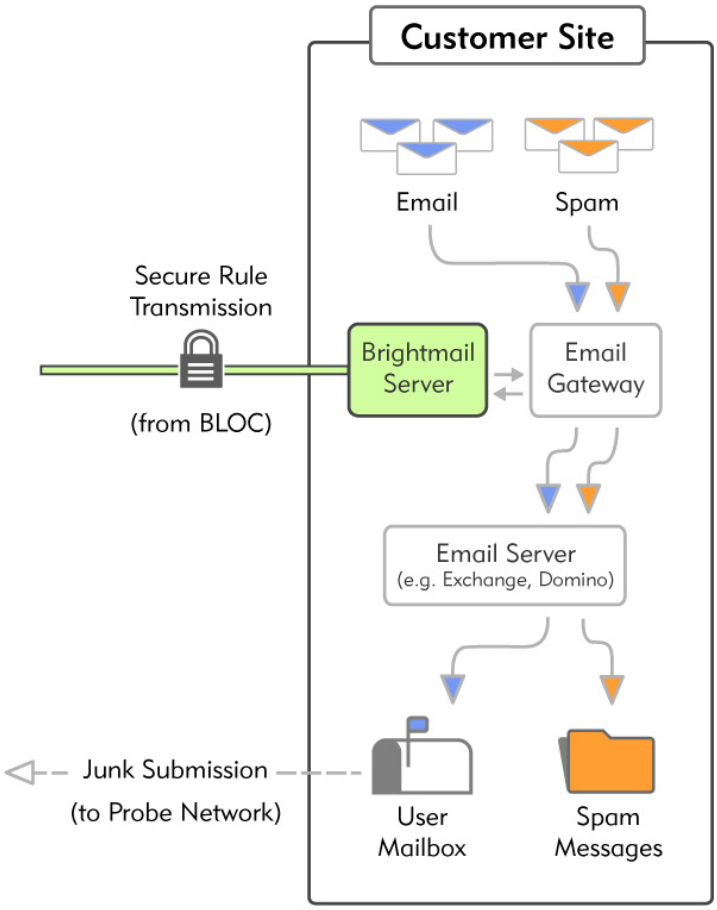
The Probe Network has a statistical reach of more than 250 million email accounts. It consists of millions of decoy email addresses that receive more than 300 million spam messages per month. The data from the Probe Network is used for the real-time creation of anti-spam rules that are propagated to Brightmail customers every few minutes - 24 hours per day. This patent protected technology is used to provide Brightmail customers with spam protection from the highly dynamic, ever changing, phenomena that spam has become.

U.S. Patent 6,052,709 (Apparatus and method for controlling delivery of unsolicited electronic email)



BLOC (Brightmail Logistics and Operations Center)

- Operates 24 hours/day - 365 days/year
- Employs state-of-the-art tools to identify new spam attacks
- Messages are automatically grouped into spam attacks and then rules automatically written against them
- QA technicians verify the rules before they are made available
- New anti-spam rule updates every few minutes
- Rules are transmitted via a secure conduit (HTTPS)



- Brightmail software is installed at the customer site
- Brightmail's extensive anti-spam rule set contains filters that automatically block identified spam attacks
- Uses sophisticated grouping algorithms and pattern matching to identify and eliminate spam as it enters the email gateway
- Updated in real-time
- Protection against spam is always current